

ROYAUME DU MAROC
.....
ADMINISTRATION
DE LA DEFENSE NATIONALE
.....
Direction Générale de la Sécurité
des Systèmes d'Information



المملكة المغربية
.....
إدارة الدفاع الوطني
.....
المديرية العامة لأمن نظم المعلومات
.....
مركز اليقظة والرصد والتصدي
للتهجمات المعلوماتية

.....
Centre de Veille de Détection et de
Réaction aux Attaques Informatiques

BULLETIN DE SECURITE

Titre	Vulnérabilités affectant plusieurs produits d'Adobe
Numéro de Référence	40231502/23
Date de Publication	15 Février 2023
Risque	Important
Impact	Important

Systemes affectés

- Adobe After Effects versions antérieures à 23.2 sur Windows et macOS
- Adobe After Effects versions antérieures à 22.6.4 sur Windows et macOS
- Adobe Connect versions antérieures à 11.4.6
- Adobe Connect versions antérieures à 12.2
- Adobe FrameMaker versions antérieures à 2020 Update 5
- Adobe FrameMaker versions antérieures à 2022 Update 1
- Adobe Bridge versions antérieures à 12.0.4
- Adobe Bridge versions antérieures à 13.0.2
- Photoshop 2022 versions antérieures à 23.5.4
- Photoshop 2023 versions antérieures à 24.1.1
- Adobe InDesign versions antérieures à ID18.2
- Adobe InDesign versions antérieures à ID17.4.1
- Adobe Premiere versions antérieures à Rush 2.7
- Adobe Animate 2022 versions antérieures à 22.0.9
- Adobe Animate 2023 versions antérieures à 23.0.1
- Adobe Substance 3D Stager versions antérieures à 2.0.0

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques
Informatiques
Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات, مديرية تدير مركز اليقظة والرصد
والتصدي للتهجمات المعلوماتية
هاتف: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني contact@macert.gov.ma

Identificateurs externes

CVE-2023-22233, CVE-2023-22237, CVE-2023-22238, CVE-2023-22239, CVE-2023-22232
CVE-2023-21584, CVE-2023-21619, CVE-2023-21620, CVE-2023-21621, CVE-2023-21622
CVE-2023-21583, CVE-2023-22227, CVE-2023-22228, CVE-2023-22229, CVE-2023-22230,
CVE-2023-22231, CVE-2023-22226, CVE-2023-21574, CVE-2023-21575, CVE-2023-21576,
CVE-2023-21577, CVE-2023-21578, CVE-2023-21593, CVE-2023-22234, CVE-2023-22244
CVE-2023-22236, CVE-2023-22243, CVE-2023-22246,

Bilan de la vulnérabilité

Adobe a publié des mises à jour de sécurité qui permettent de corriger plusieurs vulnérabilités affectant ses produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant d'exécuter du code arbitraire, de causer un déni de service, ou de contourner des mesures de sécurité.

Solution

Veillez se référer aux bulletins de sécurité d'Adobe pour l'obtention des correctifs.

Risque

- Exécution de code arbitraire
- Déni de service
- Contournement de mesures de sécurité

Référence

Bulletins de sécurité d'Adobe:

- https://helpx.adobe.com/security/products/after_effects/apsb23-02.html
- <https://helpx.adobe.com/security/products/connect/apsb23-05.html>
- <https://helpx.adobe.com/security/products/framemaker/apsb23-06.html>
- <https://helpx.adobe.com/security/products/bridge/apsb23-09.html>
- <https://helpx.adobe.com/security/products/photoshop/apsb23-11.html>

- <https://helpx.adobe.com/security/products/indesign/apsb23-12.html>
- https://helpx.adobe.com/security/products/premiere_rush/apsb23-14.html
- <https://helpx.adobe.com/security/products/animate/apsb23-15.html>
- https://helpx.adobe.com/security/products/substance3d_stager/apsb23-16.html